

## PATENT ABSTRACTS OF JAPAN

RECEIVED

AUG 30 2001

Technology Center 2600

(11)Publication number : 11-215452

(43)Date of publication of application : 06.08.1999

(51)Int.Cl.

H04N 5/765  
H04N 5/781

(21)Application number : 10-011408

(71)Applicant : SEIKO EPSON CORP

(22)Date of filing : 23.01.1998

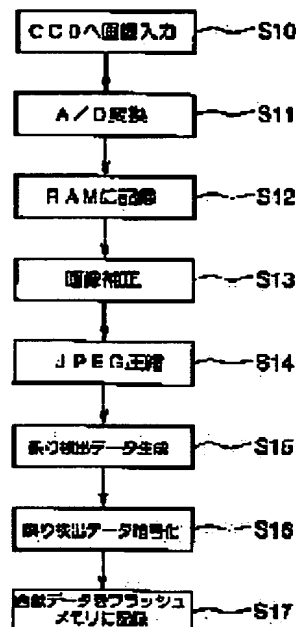
(72)Inventor : NAKAJIMA YASUMASA  
ICHIHARA SHINTARO  
MOGAMI KAZUTO

## (54) DIGITAL CAMERA AND IMAGE AUTHENTICATION SYSTEM USING THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To allow a system to confirm whether or not image data have been altered from image data at photographing.

SOLUTION: An electric signal outputted from a CCD is converted into a digital signal in a step S11. Digital data outputted from an A/D converter are stored in a RAM in a step S12. Various image corrections are applied to the data stored in the RAM in a step S13. The data corrected in the step S13 are compressed by the JPEG system in a step S14. Error detection data are generated from the compressed image data in a step S15. Error detection data are encrypted in a step S16 to obtain encrypted data. The image data and the encrypted data are stored in a flash memory as a JPEG file, in cross reference with each other in a step S17.



## LEGAL STATUS

[Date of request for examination] 09.09.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

**\* NOTICES \***

The Japanese Patent Office is not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

**CLAIMS**

---

[Claim(s)]

[Claim 1] The digital camera characterized by having a means to associate and output the photosensor which has two or more pixels, a means to change the output of the aforementioned photosensor into the image data which consists of a digital signal, the record medium which records the aforementioned image data, a means to generate error detection data from the aforementioned image data, and the aforementioned image data and the aforementioned error detection data.

[Claim 2] The digital camera according to claim 1 characterized by having a means to encipher the aforementioned error detection data.

[Claim 3] It is the digital camera according to claim 1 or 2 characterized by being able to detach [ record medium / aforementioned ] freely, and for the aforementioned image data and the aforementioned error detection data relating, and recording them.

[Claim 4] The picture image authentication system characterized by having a means to be a picture image authentication system using the digital camera given in any 1 term of claims 1-3, and to input image data and error detection data, and a means to collate the aforementioned image data with the aforementioned error detection data.

---

[Translation done.]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-215452

(43) 公開日 平成11年(1999) 8月6日

(51) IntCl.<sup>6</sup>

H 0 4 N 5/765  
5/781

識別記号

F I

H 0 4 N 5/781

5 1 0 F  
5 1 0 L

審査請求 未請求 請求項の数 4 O L (全 6 頁)

(21) 出願番号 特願平10-11408

(22) 出願日 平成10年(1998) 1月23日

(71) 出願人 000002369

セイコーエプソン株式会社  
東京都新宿区西新宿 2丁目4番1号

(72) 発明者 中島 靖雅

長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

(72) 発明者 市原 信太郎

長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

(72) 発明者 最上 和人

長野県諏訪市大和3丁目3番5号 セイコーエプソン株式会社内

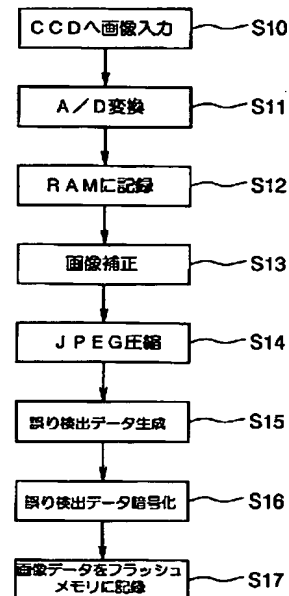
(74) 代理人 弁理士 鈴木 喜三郎 (外2名)

(54) 【発明の名称】 デジタルカメラおよびそれを用いた画像認証システム

(57) 【要約】

【課題】 撮影時の画像データから変更されたか否かを確認することのできる画像データを出力するデジタルカメラを提供する。

【解決手段】 ステップS11ではCCDから出力された電気信号をデジタル信号に変換する。ステップS12ではA/D変換器から出力されたデジタルデータをRAMに記録する。ステップS13ではRAMに記録されたデータについて各種の画像補正を行う。ステップS14ではステップS13で補正されたデータをJPEG方式により圧縮する。ステップS15では圧縮された画像データから誤り検出データを生成する。ステップS16では誤り検出データを暗号化して暗号化データとする。ステップS17では画像データと暗号化データとを関連付けてJPEGファイルとしてフラッシュメモリに記録する。



## 【特許請求の範囲】

【請求項 1】 複数の画素を有する光センサと、  
前記光センサの出力をデジタル信号からなる画像データ  
に変換する手段と、

前記画像データを記録する記録媒体と、  
前記画像データから誤り検出データを生成する手段と、  
前記画像データと前記誤り検出データとを関連付けて出  
力する手段と、を備えることを特徴とするデジタルカメ  
ラ。

【請求項 2】 前記誤り検出データを暗号化する手段を 10  
備えることを特徴とする請求項 1 に記載のデジタルカメ  
ラ。

【請求項 3】 前記記録媒体は着脱自在であり、前記画  
像データと前記誤り検出データとが関連付けて記録され  
ることを特徴とする請求項 1 または 2 に記載のデジタル  
カメラ。

【請求項 4】 請求項 1～3 のいずれか一項に記載のデ  
ジタルカメラを用いた画像認証システムであって、  
画像データおよび誤り検出データを入力する手段と、  
前記画像データを前記誤り検出データにより照合する手  
段と、を備えることを特徴とする画像認証システム。 20

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、撮影した画像をデ  
ジタルデータとして記録するデジタルカメラに関するも  
のである。

## 【0002】

【従来の技術】従来より、写真を撮影するときには、レ  
ンズから取り込まれた光がフィルムの上に照射され、化  
学反応が起きることで画像が記録されるカメラが用いら  
れている。上記のカメラでは、フィルムを現像し、印画  
紙に焼き付けることにより写真をプリントすることがで  
きる。上記の化学反応として一般に塩化銀の反応が利用  
されるため、このようなカメラによって撮影された写真  
を銀塩写真という。 30

【0003】一方、近年では CCD 等の光センサにより  
光を電気信号に変換し、それをデジタル信号に変換して  
から、フラッシュメモリ等の記録媒体に記録するデジ  
タルカメラが普及している。デジタルカメラを用いると、  
パソコン等を用いて画像の保存や様々な加工を個人で手  
軽に行えるほか、プリンタで出力することによりフィル  
ムの現像をすることなしに写真を印刷することができ  
る。プリンタの印刷品質の向上により、銀塩写真とほと  
んど区別がつかないほど品質の高い写真も印刷できるよ  
うになってきている。

## 【0004】

【発明が解決しようとする課題】しかしながら、損害保  
険等の証明写真にデジタルカメラで撮影した写真を用い  
ようとする場合に、デジタルカメラで撮影された画像は  
パソコン等により容易に加工が可能であり、銀塩写真と 50

比較して加工の跡を残さずに加工することができるた  
め、不正に加工されたいわゆる改ざんされた写真が用い  
られていても判別することが困難であり、悪用される恐  
れがあるという問題がある。

【0005】したがって、本発明の目的は撮影時の画像  
データから変更されたか否かを確認することのできる画  
像データを出力するデジタルカメラおよびそれを用いた  
画像認証システムを提供することにある。

## 【0006】

【課題を解決するための手段】本発明の請求項 1 に記載  
のデジタルカメラによれば、画像データを記録する画像  
記録媒体と、画像データから誤り検出データを生成する  
手段と、画像データと誤り検出データとを関連付けて出  
力する手段とを備える。従って、撮影時に記録媒体に記  
録された画像データが、デジタルカメラから出力後に 1  
ビットでも変更された場合には、画像データと誤り検出  
データとが不整合となるため、撮影後に画像データが変  
更されたと判断することができる。また、画像データと  
誤り検出データとの整合性がとれていれば、画像は撮影  
時のままであると判断することができる。誤り検出デー  
タを生成する方法としては、画像データのチェックサム  
を求める方法や、CRC (Cyclic Redundancy check)  
あるいは一方向ハッシュ関数 (one-way hash functio  
n) などを用いることができる。

【0007】本発明の請求項 2 に記載のデジタルカメラ  
によれば、誤り検出データは暗号化されるため、画像デ  
ータが同一の誤り検出データを得られる別の画像データ  
に変更されることや、画像データの変更に合わせて誤り  
検出データが書き換えられるのを防ぐことができる。

【0008】本発明の請求項 3 に記載のデジタルカメラ  
によれば、画像記録媒体は着脱自在であるため、画像記  
録媒体をデジタルカメラからの出力手段として用いるこ  
とができる。また、デジタルカメラから取り外した画像  
記録媒体をパソコン等により直接読取って画像データを  
入力する場合に、撮影時から変更されたか否かを判断可  
能な画像データとして出力するためには、画像データと  
誤り検出データとが画像記録媒体に関連付けて記録され  
ることが必要である。

【0009】本発明の請求項 4 に記載の画像認証シス  
テムによれば、画像データおよび誤り検出データを入力す  
る手段と、画像データを誤り検出データにより照合する  
手段とを備えるため、入力された画像データがデジタル  
カメラによって記録されてから変更されたか否かを判断  
することができる。

## 【0010】

【発明の実施の形態】以下、本発明の実施の形態を図面  
に基づいて詳細に説明する。

【0011】図 2 は本発明の実施例のデジタルカメラ 1  
を説明するためのブロック図である。制御装置 11、集  
光レンズ 12、光センサとしての CCD (Charge Coup

edDevice) 13、A/D変換器14、RAM(Random Access Memory) 15、画像データを記録する画像記録媒体としてのフラッシュメモリ16、フラッシュメモリ16の内容を外部のパソコン20等に出力するためのインターフェイス17などから構成される。制御装置11はCPUと、デジタルカメラ1の様々な制御を行うためのプログラムが記録されたROMと、入出力手段とを備える。

【0012】図1はデジタルカメラ1により撮影が行われる行程を示すフローチャートである。ユーザーがデジタルカメラ1のシャッターを押すと、ステップS10で、集光レンズ12により集光された光がCCD13に入力され、電気信号に変換される。集光レンズ12の絞りやシャッタースピード、すなわちCCD13の蓄積時間は制御装置11によって自動的に、またはユーザーの指示によって制御される。CCD13として、例えば図3に示すようにR(Red)、G(Green)、B(Blue)の原色フィルタを有する複数の画素がマトリックス状に配置されたCCD13を用いることにより、カラー画像を撮影することができる。C(Cyan)、M(Magenta)、Y(Yellow)、G(Green)の補色フィルタを有するCCDを用いる場合もある。

【0013】ステップS11では、CCD13から出力された電気信号がA/D変換器14によりデジタル信号に変換され、ステップS12ではA/D変換器14から出力されたデジタルデータが高速化のためDMA(Direct Memory Access)により制御装置11を介さずに直接RAM15のアドレスを指定して記録される。RAM15としてはセルフリフレッシュ機能をもつDRAMを用いることができる。

【0014】ステップS13では、RAM15に記録されたデータについて、ホワイトバランスの調整、補間処理、色補正などの各種の画像補正が行われる。

【0015】ステップS14では、画像記録媒体への記録枚数を多くするためにステップS13で補正されたデータをJPEG(Joint Photographic Experts Group)などの方式により圧縮し、容量の小さな画像データを生成する。JPEGはR、G、Bの各色256階調の約1670万色の画像を扱うことができ、一般に用いられる不可逆画像圧縮方法であり、圧縮率を変更することにより保存画質を調整することができる。JPEG圧縮は、制御装置11によってソフトウェア的に行うほか、高速化のために専用の回路を用いることができる。

【0016】ステップS15では、ステップS14で生成された画像データに基づいて、制御装置11により誤り検出データを生成する。誤り検出データとしては、例えばチェックサムを用いることができる。ここで、画像データ32を2進数で表したものが、図4のように示されるとする。図4のAに示すように、画像データの横方向の8ビットの桁上げなしの合計値を制御装置11によ

りそれぞれの行で計算し、それをチェックサム33とすると、画像データ32が変更された場合には、画像データ32から求められる合計値とチェックサム33が不整合となるので、画像データ32とチェックサム33とを照合することにより画像データ32が変更されたか否かを判断することができる。この場合、1行の中で2ビットが変更されると、変更されたことを検出することができないため、図4のBに示すように縦方向の8ビットについてもそれぞれの列で合計値を計算したチェックサム33をさらに用いてもよい。

【0017】また、チェックサムの他にCRC方式、一方方向ハッシュ関数等、データがオリジナルから変更されているか否かを検出することができる、データ通信等に用いられる誤り検出に関する公知の方法を本発明に適用することができる。これらの方法を用いることにより、各々の画像データに対して異なる誤り検出データを割り当てることができ、また、誤り検出データから元の画像データを再現することは非常に困難であり、実用上の問題は無いといえる。

【0018】ステップS16では、チェックサム33等の誤り検出データが解析されたり容易に書き換えられたりしないように、制御装置11により暗号化して暗号化データ34とする。暗号化の方法としては、公開鍵と秘密鍵を用いるRAS方式など、公知の方法を用いることができる。秘密鍵で暗号化した暗号化データ34は、秘密鍵と対になった公開鍵を用いて解読することができる。秘密鍵はデジタルカメラ1内に記憶されており、他人に知られてはならない。また、ユーザーが秘密鍵を知らなくてもよい。しかし、公開鍵から秘密鍵を求めることは非常に困難である。これにより、画像データ32が同一のチェックサム33を得られる別の画像データに変更されることや、画像データ32の変更に合わせてチェックサム33が書き換えられるのを防ぐことができる。

【0019】ステップS17では、画像データ32と暗号化データ34とを一体にJPEGファイル30として画像記録媒体としてのフラッシュメモリ16に記録する。フラッシュメモリ16は通電し続けなくても一旦記録した内容を保持することのできる書換え可能な記録媒体であり、デジタルカメラ1に内蔵されるか、あるいは着脱自在にデジタルカメラ1に取り付けられている。JPEGファイル30は一般に図5に示すようにデータ長、圧縮率等の情報を含むヘッダ部31と、画像データ32とから構成される。デジタルカメラ1によって記録されるJPEGファイル30の場合は、撮影日やシャッタースピード等の撮影条件等の情報もヘッダ部31に記録することができる。本実施例では、ヘッダ部31に暗号化データ34を更に加えて記録している。

【0020】フラッシュメモリ16がデジタルカメラ1に内蔵されていて、取り外しが不可能な場合には、フラッシュメモリ16には暗号化データ34等の誤り検出デ

10

20

30

40

50

ータを含まないJ P E Gファイル30を記録しておき、インターフェイス17を介して外部のパソコン20に出力する段階で誤り検出データを生成し、J P E Gファイル30のヘッダ部31に付加して出力することも可能である。なお、パソコン20からデジタルカメラ1に画像を転送できるようになっている場合は、J P E Gファイル30のヘッダ部31等により区別して、再度パソコン20に転送するときには誤り検出データを付加しないようにする必要がある。

【0021】一方、フラッシュメモリ16がデジタルカメラ1から着脱自在で、その内容をパソコン等によって読み取り可能な場合、あるいはデジタルカメラ1自体に画像を修正する機能が備えられている場合には、画像データと誤り検出データとを一体に出力するためには画像データがフラッシュメモリ16に記録される段階で、同時に誤り検出データが記録されている必要がある。

【0022】また、図1に示す本実施例のフローチャートでは、ステップS13の次にステップS14で画像データをJ P E G圧縮し、その後にステップS15、S16を実行し、誤り検出データの生成と暗号化を行ったが、ステップS13の次にステップS15、S16を実行し、そのあとにステップS14で画像データをJ P E G圧縮することも可能である。

【0023】上記のようなデジタルカメラ1と、デジタルカメラ1から出力された画像データを入力する手段を備えるパソコン20と、デジタルカメラ1によって記録された画像データが変更されたか否かを判定するためにパソコン20等のコンピュータにインストールされた認証プログラムとによって画像認証システムが構成される。

【0024】パソコン20に画像データと誤り検出データを入力する手段としては、シリアルケーブル18等を介してデジタルカメラ1のインターフェイス17と接続してフラッシュメモリ16内のJ P E Gファイルをパソコン20に転送する方法や、フラッシュメモリ16が着脱自在でパソコン20と互換性のある形式でフォーマットされている場合には、アダプタを介してフラッシュメモリ16に記録されたJ P E Gファイル30をパソコン20で直接読み取ることも可能である。

【0025】J P E Gファイル30のヘッダ部31内の暗号化データ34がデジタルカメラ1内で秘密鍵によって暗号化されている場合、認証プログラムは公開鍵を用いることにより、秘密鍵によって暗号化されたことを確認すると同時に暗号を解読することができる。解読された誤り検出データと、画像データとを照合することによって、誤り検出データが生成された時点から画像データが変更されているか否かを判断することができる。暗号化データ34が存在しない、暗号化データ34が公開鍵で解読できない、解読された誤り検出データと画像データとが不整合である場合には、その画像データは本発明

実施例のデジタルカメラ1で撮影されたものではないか、撮影後に変更されたものとみなされる。

【0026】したがって、本発明実施例の画像認証システムを使用する場合、写真の提出者は、デジタルカメラ1から出力して変更を加えていない画像データを含むファイル（本実施例ではJ P E Gファイル30）をフロッピー等の記録媒体に記録したもの、あるいは着脱可能な記録媒体であるフラッシュメモリ16をデジタルカメラ1から取り外したものを、印刷した写真と共に相手の求めに応じて提出する。受け取り側は、パソコン20にインストールされた認証プログラムを用いて受け取ったファイルを読み込んで調べることにより、そのファイルの画像データがデジタルカメラ1から出力された時点から変更されていないというを確認することができる。

【0027】また、認証プログラムにJ P E Gファイル30等の画像データの画像を表示する機能をもたせることにより、印刷された写真と表示された画像が同一であることを確認することができる。

【0028】以上、実施例によって説明したように、本発明のデジタルカメラおよびそれを用いた画像認証システムを用いることにより、デジタルカメラで撮影した写真が撮影時から変更されていない、改ざんされていない、オリジナルのものであることを確認することができる。

【0029】上記の実施例では、J P E G圧縮したものを画像データとして画像記録媒体に記録したが、本発明は他の圧縮方法で圧縮したものや、無圧縮のデータを画像データとして記録したものにも適用できる。また、誤り検出データをJ P E Gファイルのヘッダ部に記録したが、本発明としては誤り検出データは画像データのどの位置にあってもよい。画像データが無圧縮であるか、可逆圧縮されたものであるか、あるいは不可逆圧縮されたものであるかに関わらず、電子すかしの技術により、肉眼では判別できないように誤り検出データの情報を画像データの内部に含ませることも可能である。

【0030】また、本実施例では誤り検出データと画像データとを一体にJ P E Gファイルとして記録したが、誤り検出データを別ファイルとして記録し、画像データに関連付けてもよい。

【図面の簡単な説明】

【図1】本発明の実施例におけるデジタルカメラにより画像を記録する手順を示すフローチャートである。

【図2】本発明の実施例によるデジタルカメラを示すブロック図である。

【図3】本発明の実施例によるデジタルカメラに用いられるCCDを示す模式図である。

【図4】本発明の実施例による画像データのチェックサムを算出する方法を説明するための図である。

【図5】本発明の実施例による画像データと誤り検出データの記録方法を説明するための図である。

## 【符号の説明】

1 デジタルカメラ

11 制御装置

12 集光レンズ

13 CCD (光センサ)

14 A/D変換器

15 RAM

16 フラッシュメモリ (画像記録媒体)

\* 17 インターフェイス

18 接続ケーブル

20 パソコン

30 JPEGファイル

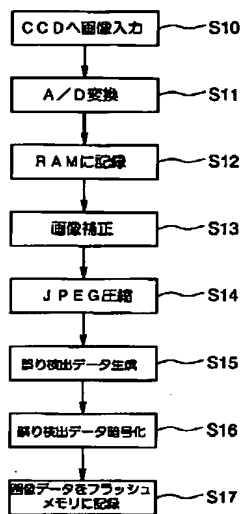
31 ヘッダ部

32 画像データ

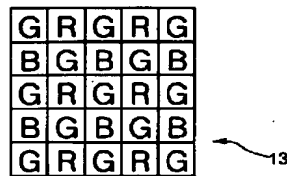
33 チェックサム (誤り検出データ)

\* 34 暗号化データ (誤り検出データ)

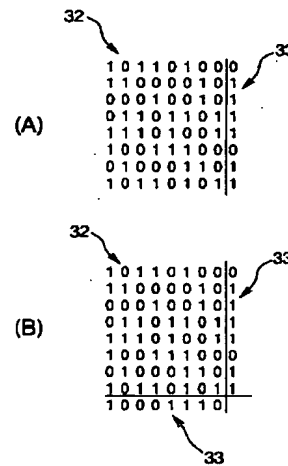
【図1】



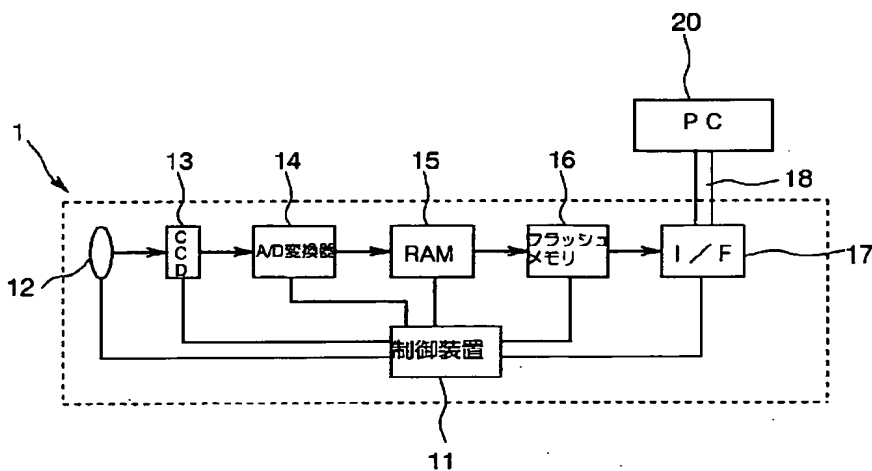
【図3】



【図4】



【図2】



【図5】

